Deloitte.

The Deloitte On Cloud Podcast

David Linthicum, Managing Director, Chief Cloud Strategy Officer, Deloitte Consulting LLP

Title: **Got cloud problems? Look to strategy and process fixes for solutions**

Description: To be sure, cloud is a boon to organizations that make the leap, but, as with any technology, there are bumps along the road to implementation. In this episode, David Linthicum talks with Techstrong Group's Mike Vizard about how companies can address three particularly vexing issues: multicloud complexity, cloud cost management, and cloud security. Mike's advice is to develop a sound multicloud cloud strategy, treat cloud as a strategic investment, and view security as a process, not a problem.

Duration: **00:24:48**

David Linthicum:
Hey, guys. Welcome back to the On Cloud Podcast. Today on the show I am joined by Mike Vizard, the chief content officer at Techstrong Group. Mike, welcome to the show.

Mike Vizard:
Hey, guys. Thanks for having me.

David Linthicum:
So, Mike is, as we mentioned, the chief content officer at Techstrong Group, publisher of DevOps.com, Security Boulevard, Container Journal, and Digital DXO. Man, you're hitting all the trends. Tell me how you got into this.

Mike Vizard:
Well, I've been doing this for a long time, but I was actually just kind of walking down the street, minding my own business when Techstrong Group, who I contributed to a lot, had a little re-org of their own and their chief content officer spot became open. And I've been vice-president of editorial for places like Ziff Davis and editor-in-chief for InfoWorld and CRN back in the day, so it's something I'm well-versed in and pretty familiar with how to operate editorial functions.

David Linthicum:
Yeah, I was just thinking before we got on the podcast. I was stalking your LinkedIn today, trying to figure out how long we've known each other and where we first met, because in tech media everybody moves around a ton. And it seems like—I know I met you in person, probably on a road show back in my CTO days. But it's just kind of funny to see the amount of knowledge that's within the technical press, that's even more so than people who are working for the technology companies, and even some of the technology advisory stuff that's out there. So, you guys seem to see it all and have a good perspective, certainly as good as the analysts. Would you agree with that?

Mike Vizard:
Yeah, I think before Covid we were all on the same trade show traveling circuits and conferences. And a lot of the guys in the tech media are some of my best friends simply because we all leave our houses and get on a plane on Monday and go somewhere and hang out for a few days, and then we go home again. Of course, it's not quite like that anymore, but maybe someday we'll all have a beer together somewhere.

David Linthicum:
Yeah, really. It's funny how everybody kind of takes in this—certainly in the tech press takes a step to the right about every five years. And it's funny how that whole thing has evolved. I remember large magazines and going to the magazine rack every day, and—at least I did every day, and look at the different technology publications to keep up. Now it's completely online and different ways of producing the information videos podcasts such as this, things like that. So, what do you think has been the most profound change in the technology media space say in the last ten years, besides the Covid stuff, just kind of a shift or a trend?

Mike Vizard:
I think overall, it's much like what happened in the other news cycles. It's 24/7 now in IT. It used to be you would get—InfoWorld would arrive hopefully on Tuesday or Wednesday with copy that was written the previous Wednesday and Thursday, and hopefully it was still relevant by the time it got there. Now we take it for granted that everything is being covered in the moment, and the minute something happens it's all over the place, and if it's big enough, everybody knows about it. So, to me it's the instant nature of the news cycle has changed all our jobs to that model. You're almost on call now, I'm sure, all the time, with reporters calling you up out of the blue going, "Hey, this happened; what do you think?" And as a writer, you never know what shoe is going to drop next.

David Linthicum:
Yeah, it's a challenge to keep up, but like I said, it's an exciting time. So, speaking of cloud computing in general, and technology in general, and DevOps, and the way security is evolving, things like that, what do you see as the new trends in 2022? What do you think we're going to be focused on toward the middle and the end of this year?

Mike Vizard:
I think there's a lot of conversation going on now about multicloud versus trying to standardize on a single cloud. If I think back for the last two years, CIOs especially have been trained to kind of reduce the number of vendors that they deal with, so they're always trying to standardize on something and people want them to sign these enterprise-level contracts. But we've seen this wave of outages and they've affected everybody, and I think a lot of organizations are now thinking about not multicloud as something that happened by accident because a bunch of developers went out and decided to use a different cloud platform, but it's now going to be an actual strategy. The idea is to optimize the right workload for the right cloud, and then if there's an issue be able to move it if we need to quickly, or at least have a backup instance of that app running somewhere that we can fire up immediately. So, in my mind, resiliency is going to be the big issue as it relates to the cloud in 2022.

David Linthicum:
Yeah, it's resiliency and it's also spreading the risk. In other words, I don't see too much of a movement where we're going to keep copies of the same workload applications and data in one cloud and then another cloud which is going to be something different than the cloud we're in. And there was some discussion of that when we started looking at some of the outages. We're going to be able to failover from one cloud brand to the other. But when you look at that it gets expensive pretty quick in maintaining these two workload balances. However, I do see—and I think this is more to your point—that we're going to start spreading the risk, in other words, in putting different workloads in different times in different clouds in order to in essence have a different option.

If, for example, the cloud provider isn't providing the same standard of services, they're just having too many outages, having too many quality problems, support problems, the points of presence are going down, network issues, things like that, it would provide us with the ability to immediately shift over to another cloud provider because we already have that onboarded and we have the monitoring and management tools and security tools to make that happen. Is that something you think we're thinking about well? Or should we be doing this A to B kind of active/active failover system, or just keeping around different options?

Mike Vizard:
I think it's going to have to be more along the line of the options, because the truth of the matter is CIOs and CTOs in these organizations don't always have the political power to force any kind of standardization. There are developers within their organizations in different business units that are doing whatever

they think is best or most interesting to them. I think the IT organization then has to come in behind that and say, "Okay, well, if that's a given, how would we make that more resilient by creating some other cloud platform that we could fire up another instance of that application on quickly if we needed to?" And they're going to have to think about it in those terms.

I think the ultimate goal would be to get to something that felt like a unified console to help manage multiple clouds. I think part of the reason that we're talking so much about the expense of cloud these days is when you look at it, it's not the cloud platform itself that's the cause of the expense. It's that each of them has a different management framework and each of those management frameworks requires me to go get somebody who knows how to operate those management frameworks and then my cost of labor goes up.

So, I'm thinking that in addition to resiliency, maybe the second part of this issue is how do you achieve resiliency in a way that contains those costs by providing some set of centralized tools that can be used across multiple clouds? We, of course, have been talking about hybrid cloud forever and a day. I'm not quite sure we're ever going to get to that perfect hybrid cloud. But I think we need to simplify the management frameworks.

David Linthicum:
Yeah, and I think that what you're getting at is we have a complexity and a heterogeneity problem, and so we have to be able to get at that and solve it so we can operationalize these systems. When you get into the different talents that are needed in managing these cloud-native services and then keeping different humans around that are able to understand how those things are going to be managed and monitoring, when you get into these very complex, these very heterogeneous multicloud deployments, we just can't operationalize them on the budgets that we're looking to make.

And, so, we have to consider how we're going to abstract the services, how we're going to leverage common management and monitoring services, common security between the various cloud providers, common governance between the cloud providers. And when you look at people who are deploying multicloud today, those are typically not the discussions they're having. They're securing these things with their cloud-native security services that come with a particular cloud brand, same with governance, same with management and monitoring, same with application development, DevOps, infrastructure, things like that.

And I don't think—and I think to your point as well—we can't afford to separate those things out. We have to manage a multicloud as a holistic system, in other words look for the common services, the commonality of infrastructure, the ability to leverage technology as a force multiplier to run across these various cloud providers and get to a point we're able to operationalize these systems at a cost that is about the same or even less than we could the more traditional systems. Am I too optimistic?

Mike Vizard:
I think that's the goal. It's going to be a lot harder to do than say. And I think it's getting worse because we are playing around now more with these cloud-native technologies. So, we're running complex microservices-based applications using containers running on Kubernetes platforms. We don't really know the people or have enough of those types of people to manage that effectively, and yet we have tons of these legacy monolithic applications that are running today, that aren't going away anytime soon, and some of them might get peeled off as a microservice but a very few, small number of that will occur over the years, not in months.

And we're going to wind up with a situation where we're going to have—I don't know; I'll take a guess. Eighty percent of the workloads will be still legacy, monolithic, running on virtual machines, and eventually 20 percent will be microservices-based Kubernetes that are more complex. They may be more resilient but they're harder to manage. I think that that just says that in the short term the cost of managing the cloud is going to go up. It just can't be avoided. Maybe a couple of years out we'll reduce those costs again, but I don't think that we're going to get there and maybe we should have a realistic conversation about what is the real cost of the cloud.

David Linthicum:
Yeah, and I think we're having those conversations now as people are looking at cloud computing as a strategic investment that the companies are making. There's a few consistent things that are happening. Number one, we're spending way more on cloud than we thought we would, and so cloud was evidently going to be sold as something that's going to reduce the costs and certainly the operational costs of running a traditional business. So, let's move in that direction.

However, if we think in how we value cloud computing, it's really about valuing this in terms of a strategic value to the business, the ability to become innovative, the ability to compress the time that it takes to build products and services, the ability to delight a customer with some of the digital enablement they have out there. And, so, the metrics become a little foggy in terms of how you look at how cost actually relates back to cloud-based systems. Do you think that we're going to adjust our thinking? Or do you think that this is still going to be a bit of a letdown when people see what they have to spend operationally on cloud computing versus perhaps what they were told ten years ago?

Mike Vizard:
I think people are adjusting to that. I think they've already seen it post-Covid. They saw the workloads shift over there more rapidly, and I think people are more generally aware. The balance against that is how much can we rely on automation and hopefully someday maybe AIOps to enable us to manage all this stuff at scale within the current cost parameters? But I feel it's going to take a little bit for those automation frameworks to really kick in and be that reliable. So, I think eventually we'll get back down to that cost level using automation and some of these more advanced frameworks, but there's going to be a bump in the middle here and I think people should figure out what that cost structure is and be realistic about it. You're just not going to be able to manage the number of workloads that we want to run in this so-called business transformation age with the same number of people you have today. It's not going to happen.

David Linthicum:
Yeah, absolutely. I think we're just going to end up spending more money, but if you think about it also, too, we may not have a choice. If the market is shifting to cloud computing, then we're not necessarily investing innovation and R&D spending on traditional systems. And, so, if traditional systems aren't getting invested in and therefore, they're not improving as fast as they should, certainly as fast as cloud, and certainly when there are systems—certainly in the AI we're seeing this. There's more technology that's in the cloud, there's better technology in the cloud, so there's almost like a forced migration into

cloud computing. And, so, if you look at the cost stuff and the cost justification—that's certainly legitimate, that people are able to do that—at the end of the day there may not be a choice.

The market's making the choice for you. And I think enterprises are a bit concerned about that. But if you think about it, we've seen this in the past movement to the PC, distributed computing, off of timeshare systems, things like that. And, so, technology evolves, we evolve as well, and how people leverage technology is going to change over time. And in essence, you have to go along with the technology shifts. You can't buck the trend. So, there really is no place for a business that wants to kind of hold firm with their traditional technology if they expect to grow and expect to thrive in a market moving forward. Am I being too pessimistic?

Mike Vizard:
No, but I think there's one other factor to consider here, is to what degree are we going to lean more on managed services or so-called as-a-service platforms that we're seeing from the various server vendors out there that are essentially a managed service? And what we're seeing is the cloud service provider or the manufacturer of the server wants to take on the role of IT operations. And if that's the case, does that enable people to spend more time and money on building and deploying applications and software? And the internal IT team will essentially move up the stack and maybe the underlying hardware becomes increasingly automated by somebody else.

David Linthicum:
Absolutely. And I think, ultimately, those are things that we kind of need to factor in in terms of how we expect cloud computing to perform and how to leverage it correctly. So, let's shift gears just slightly and talk about it more in terms of what's going to happen in 2022 around cloud security. And obviously that's front and center to all people who are making IT decisions and certainly people who are leveraging cloud computing. Cloud security is first and foremost, probably even more so than traditional systems. So, where are we evolving around the cloud security shift in 2022 and what are the topics that are going to be most important? What are you going to be writing about this year?

Mike Vizard:
Looking into 2022, I think cloud security is going to be a major issue going forward because we are seeing just tons and tons of misconfigurations. And I know that the cloud platform providers will tell you that the platform is secure, and it sure is, but they have this shared responsibility model and everything above the infrastructure is your responsibility.

Well, a lot of organizations are just letting developers with no security expertise provision infrastructure, put workloads up in the cloud, and then, lo and behold, we're surprised when a port's left open and data's being exfiltrated because the cybercriminals are smarter than ever, and we really don't have a mature set of processes for this.

It's amazing that we have gotten this far without considering this issue more aggressively, and I think this whole conversation around software supply chain is part of that. DevSecOps is part of that. Even API security is part of that. And it's the whole issue of how do we kind of lock down these environments in a way that doesn't necessarily force us to slow down the rate at which we're building and deploying applications, but we've got to take a step back and figure out how to make these environments more secure because we're having kind of one of these Ralph Nader moments where we were unsafe at any speed, right?

David Linthicum:
Moving forward, what I think is going to be important is to evaluate exactly what your needs are and the ability to get a minimum viable security thing in place, because the answer can't be that we can never be too secure. You can be too secure. You can be spending too much money on security based on what you're securing.

And I think the thinking needs to shift that way because we only have a limited amount of resources, money in this case, a budget, and I think we have a tendency not to spend that as strategically wise as we can when we're dealing with security.

And, so, the IT groups I think need to back up a bit—and certainly what you said is true—evaluate the workloads and see which kinds of security mechanisms need to be put in place, and—but really get down to what the risks are and what the cost of the risk is. And that doesn't mean you ever want a data breach or have ransomware in place but putting steps in place to deal with the majority of risks, to reduce the risk as much as possible, understanding it'll never be to zero. And I think we're just kind of too reactionary in the last ten years in terms of cloud security. And this year it's going to be about picking our battles and the ability to adjust the solutions that are more aligned with the requirements. Am I thinking wrongly?

Mike Vizard:
No, I think you're on it. I think we need to think about security as a process. It's not something you buy; it's something you achieve, and you do that by enforcing a set of policies and processes that are manageable and dictated by what is the value of the thing being secured. We in the real world don't put cheap jewelry in a very expensive bank safe, right? We kind of say we're going to put our most valuable stuff in the bank and other stuff will be in a lockbox at home, right? It's that kind of thinking. We need to kind of right-size the security spend for the risk at hand.

David Linthicum:
Do you think that moving to these different new technologies—maybe not new as much anymore, certain containers and Kubernetes clusters, the ability to deal with serverless, low-code and no-code computing, and really things I'm sure you're writing about a lot because they're popular topics in the tech press out there—is going to get us into more security trouble? Because, in essence, the technology seems to lead the security solutions, we have a tendency not to think critically about security until we have these solutions in place.

It just seems to follow the technology, again, versus leading to the technology. Are we going to see some folks getting into security issues, causing breaching, increasing the risk because we're chasing the new shiny stuff and not necessarily looking at how we're going to secure it? It's almost better to stay back a couple years, clicks in terms of following the hype cycle, because we understand the security solutions will be there. If we're going to lead the edge, then we're going to end up bleeding with some security issues. What are your thoughts on that?

Mike Vizard:
I think there's two sides to this, and one is a negative and one's a big positive. So, the negative is that, yes, these things are more complex and there's more moving parts, and the opportunities to make mistakes are much higher, so the probability that there's going to be an issue is almost absolute. The second thing that people may not be appreciating just yet is that today, if I have a problem with an application that's monolithic, I've got to patch that thing. And the reason we have so many vulnerabilities that don't go patched is because it's hard.

It's difficult. It takes a lot of effort and a lot of time, and the people who built the application may not be around anymore. If you look at a modern application that's built on containers and microservices, it's much more modular. So, when there is a piece of offending code that is the team—vulnerable or, in the case of Log4j or something like that, became vulnerable overnight, I can rip and replace the containers and the microservices much more easily and just update that portion of the application. So, we may wind up with more secure applications eventually because our muscle memory and our processes for remediating the vulnerabilities is going to be a lot better.

David Linthicum:
So, in other words, new technology provides us with opportunities to become more secure.

Mike Vizard:
Yeah, I think so. I think that'll be a backend benefit. I don't think we'll see that immediately, but my bet is if we're sitting here having this conversation next year, one of the reasons that more organizations will be shifting to so-called cloud-native technologies will be because they are easier to fix.

David Linthicum:
Yeah, and I think one of the trends that we're seeing as we're starting to build applications differently, certainly using containers and other technologies, is that we're making things that are more distributed, and the ability to decouple these applications actually provides you with the ability to secure them better. I do notice that when you're looking at security engineering.

If it's a monolithic application where the data is tightly coupled to the application, it's going to be more secure than if you have the applications that are decoupled from the data—and by the way, the applications are partitioned into three or four different entities that can be protected in different ways. In other words, we have different security options because we're able to divide the application up to its function and the data up to its function and not necessarily held back by something that was probably incorrectly engineered 10, 20 years ago. What are your thoughts on that?

Mike Vizard:
I think that developers don't know how to talk to security people, and I don't think security people, for that matter, know how to talk back to the developers. They just live in different lands and different languages. But what you're describing is a major benefit for all IT organizations. It's just that developers are so focused on speed that it never occurs to them to go back to the security guys and go, "Hey, by the way, one of the downstream benefits of shifting to this is going to be that when there is an issue—and there's always going to be issues—we can respond more jointly and faster."

And this will be a huge benefit for the security guy because you're not going to be running people around banging people to do patches for things and having developers look at you because maybe they didn't use that code or they did use that code, they don't know, it's all over the place. It'll just—the heavy lifting required will be so much less that people won't fight you over it. They'll be like, "Sure, we'll rip and replace that. It'll take us a couple of days maybe." But right now, it takes weeks and months.

David Linthicum:
Yeah, I think that's great advice. So, Mike, where can we find your stuff on the web? It looks like you have a lot of assets out there. You want to go through them really quick?

Mike Vizard:
Well, we have DevOps.com and Security Boulevard are probably the two primaries, and then Container Journal. We just launched Digital CXO, which is trying to bridge the divide between C-level execs that exist between say the CIO and the CTO and the rest of the C-level suite. We want to have a conversation about how they collaboratively come together to drive something of value for the business that's driven by IT.

So, this is our first C-level title; it's a major investment for us. We're actually having a big conference in April up in Cocoa Beach at the Kennedy Space Center. We're going to invite some folks to talk about this issue and others. And we're also now sponsoring a series of dinners that we're going to have around the country. So, we're putting a lot of money behind this thing, so hopefully this time next year everybody will be at least aware of Digital CXO. But it's our little baby at the moment.

David Linthicum:
Yeah, everybody out there who's listening to this podcast follow Mike. He's really good at creating thoughtful articles and content and putting things into perspective. And, so, it's enough commentary and thinking around the emerging trends and it's something you should follow. I don't follow columns and blogs; I follow people. Mike would definitely be the top five in the country right now that I would consider as kind of a leader in terms of innovating how people need to follow this technology path and doing so with the right amount of advisory. So, keep up with Mike. It's good that he's out there, and it's great to talk to you again, Mike.

Mike Vizard:
Good talking to you. Right back at you for those kind words because I follow you for all the same reasons. But thanks for having me on the show.

David Linthicum:
Well, thank you very much. So, if you enjoyed this podcast, make sure to like us, rate us, and subscribe. You can also check out our past episodes including those hosted by my good friend Mike Kavis. Find out more about Deloitte Cloud Podcasts at DeloitteCloudPodcast.com. If you'd like to contact me directly, you can e-mail me at DLinthicum@Deloitte.com. That's L-I-N-T-H-I-C-U-M. So, until next time, best of luck in your cloud journey. You guys stay safe. Take care.

David Linthicum
If you enjoyed this podcast, make sure to like us, rate us, and subscribe. You can also check out our past episodes, including those hosted by my good friend, Mike Kavis. Find out more at “deloitte cloud podcast .com” all one word. If you'd like to contact me directly, email me at dlinthicum@deloitte.com. Until next time, best of luck with your cloud journey, and stay safe!

Operator:
This podcast is produced by Deloitte. The views and opinions expressed by podcast speakers and guests are solely their own and do not reflect the opinions of Deloitte. This podcast provides general information only and is not intended to constitute advice or services of any kind. For additional information about Deloitte, go to Deloitte.com/about.

Visit the On Cloud library
www.deloitte.com/us/cloud-podcast